CLAIMS

What is claimed is:

1. A descrambler integrated circuit (IC) adapted to receive scrambled digital content, a message and an encrypted descrambling key, comprising:

a local memory to store a unique key;

a first process block to decrypt a message using the unique key to produce a key;

a second process block using the key to decrypt the encrypted descrambling key and to recover a descrambling key; and

a descrambler using the descrambling key to descramble the scrambled digital content and to produce digital content in a clear format.

2. The descrambler IC of claim 1, wherein the unique key is loaded into the local memory during manufacture of the descrambler IC.

3. The descrambler IC of claim 1, wherein the second process block is a finite state machine.

4. The descrambler IC of claim 1, wherein the message is a mating key generator that comprises an identifier of a supplier of the scrambled digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider.

5. The descrambler IC of claim 4, wherein the mating key generator further comprises an identifier that identifies a provider of a system that enables

transmission of the scrambled digital content and the mating key generator message to the descrambler IC.

6. The descrambler IC of claim 5, wherein the mating key generator further comprises (i) an identifier that identifies a conditional access (CA) system provider over which the scrambled digital content and the mating key generator is transmitted, and (ii) a mating key sequence number.

7. The descrambler IC of claim 1, wherein the first process block and the second process block are logic operating in accordance with one of the following: Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Triple DES.

8. The descrambler IC of claim 1, wherein the unique key is a one-time programmable value that cannot be read or overwritten once programmed.

9. A descrambler integrated circuit (IC) adapted to receive scrambled digital content, a mating key generator and at least two encrypted descrambling key, comprising:

a local memory to store a unique key;

a first process block using the unique key to encrypt the mating key generator and to produce a key;

a second process block using the key to decrypt a first encrypted descrambling key and to recover a first descrambling key;

a third process block using the key to decrypt a second encrypted descrambling key and to recover a second descrambling key; and

a descrambler to descramble the scrambled digital content using both the first descrambling key and the

second descrambling key in order to produce digital content in a clear format.

10. The descrambler IC of claim 9, wherein the unique key being loaded into the local memory during manufacture of the descrambler IC.

11. The descrambler IC of claim 9, wherein the mating key generator comprises an identifier of a supplier of the scrambled digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider.

12. The descrambler IC of claim 9, wherein the mating key generator comprises an identifier that identifies a provider of a system that enables transmission of the scrambled digital content and the mating key generator message to the descrambler IC.

13. The descrambler IC of claim 9, wherein the mating key generator message comprises (i) an identifier that identifies a conditional access (CA) system provider over which the scrambled digital content and the mating key generator is transmitted, and (ii) a mating key sequence number.

14. The descrambler IC of claim 9, wherein the first process block, the second process block and the third process block are logic operating in accordance with a Data Encryption Standard (DES).

15. The descrambler IC of claim 9, wherein the unique key is a one-time programmable value that cannot be read or overwritten once programmed.

16. A descrambler integrated circuit (IC) comprising:

a local memory to store a unique key;

a first process block, using the unique key, to perform at least two successive cryptographic operations on a first mating key generator in order to produce a first key;

a second process block, using the first key, to perform at least two successive cryptographic operations on a second mating key generator in order to produce a second key;

a third process block, using the first key and the second key, to decrypt a first encrypted descrambling key to recover a first descrambling key;

a fourth process block, using the first key and the second key, to decrypt a second encrypted descrambling key to recover a second descrambling key; and

a descrambler to descramble the scrambled digital content using both the first descrambling key and the second descrambling key in order to produce digital content in a clear format.

17. The descrambler IC of claim 16, wherein the first process block and the second process block operate in accordance with Triple Data Encryption Standard (3DES).

18. The descrambler IC of claim 16, wherein the third process block and the fourth process block operate in accordance with Triple Data Encryption Standard (3DES).

19. The descrambler IC of claim 16, wherein the third process block, using the first key, performing at least two decryption operations and at least one

encryption operation on the first encrypted descrambling key in succession.

20. The descrambler IC of claim 16, wherein the second mating key generator comprises a first field that provides copy controls and a second field that identifies incoming content to which the copy controls apply.

21. The descrambler IC of claim 19, wherein the second mating key generator further comprises a third field including a value that identifies the number of times the digital content can be copied.

22. The descrambler IC of claim 16 being in communication with a smart card to receive the first mating key generator and the second mating key generator are provided from the smart card.

23. A descrambler integrated circuit (IC) adapted to receive scrambled digital content and to descramble the scrambled digital content, comprising:

a first process block to encrypt a message using a unique, one-time programmable key to produce a first key;

a second process block to receive an encrypted second key and, using the first key, to decrypt the encrypted second key in order to recover the second key in a non-encrypted format; and

a descrambler using the second key in the non-encrypted format to descramble the scrambled digital content and to produce digital content in a clear format.

24. The descrambler IC of claim 23, wherein the encrypted second key is an encrypted service key associated with at least one selected tier of service.

25. The descrambler IC of claim 23, wherein the encrypted second key is an encrypted descrambling key from a smart card in communication with the descrambler IC.

26. The descrambler IC of claim 23, wherein the message encrypted by the first process block is a mating key generator being a message that comprises an identifier of a manufacturer of a digital device employed with the descrambler IC.

27. The descrambler IC of claim 26, wherein the mating key generator encrypted by the first process block further comprises a service provider identifier, and a conditional access (CA) provider identifier.

28. A descrambler IC comprising:

a local memory to store a unique key;

a first process block, using the unique key, to encrypt a message received by the descrambler IC, the first process block to produce a user key;

a second process block, using the user key, to decrypt the encrypted user key received by the descrambler IC, the second process to recover a copy protection key from the encrypted user key;

a third process block, using the unique key, to decrypt an encrypted descrambling key received by the descrambler IC, the third process block to recover the descrambling key in a clear format;

decryption logic, using the descrambling key in the clear format, to decrypt encrypted digital content received by the descrambler IC, the decryption logic to recover the digital content in a clear format; and

encryption logic, using the copy protection key, to re-encrypt the digital content in the clear format to

produce encrypted digital content for transmission from the descrambler IC.

29. The descrambler IC of claim 28, wherein the first process block to encrypt the message being a copy protection key generator that comprises that comprises an identifier of a supplier of the encrypted digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider.

30. The descrambler IC of claim 28, wherein the mating key generator further comprises an identifier that identifies a provider of a system that enables transmission of the encyrpted digital content and the copy protection key generator to the descrambler IC.

31. The descrambler IC of claim 30, wherein the copy protection key generator further comprises (i) an identifier that identifies a conditional access (CA) system provider over which the scrambled digital content and the mating key generator is transmitted, and (ii) a copy protection status to provide content management controls that comprise at least one of (i) a control to indicate whether or not the incoming content can be copied, (ii) a control to indicate a number of times for playback of the digital content, and (iii) a control to indicate a date/time of playback of the digital content.

32. A descrambler integrated circuit (IC) adapted to receive scrambled digital content, a message and an encrypted descrambling key, comprising:

a local memory to store a unique key;

a first process block controlled by a non-CPU based state machine to decrypt a message using the unique key to produce a key;

a second process block controlled by a non-CPU state machine using the key to decrypt the encrypted descrambling key and to recover a descrambling key; and

a descrambler using the descrambling key to descramble the scrambled digital content and to produce digital content in a clear format.